PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Geoffrey S. Strongin	Conf. No. 6696
	Examiner: ELLEN C. TRAN
Serial No.: 09/853,465	
	Group Art Unit: 2134
Filed: May 11, 2001	
	Att'y Docket: 2000.039500
For: CRYPTOGRAPHIC COMMAND-RESPONSE ACCESS TO A MEMORY IN A PERSONAL COMPUTER SYSTEM	Customer No. 23720

REPLY BRIEF

MAIL STOP AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This paper is submitted in response to the Examiner's Answer dated July 20, 2006, for which the shortened two-month date for response is September 20, 2006.

If an extension of time is required to enable this paper to be timely filed and there is no separate Petition for Extension of Time filed herewith, this paper is to be construed as also constituting a Petition for Extension of Time Under 37 CFR § 1.136(a) for a period of time sufficient to enable this document to be timely filed.

It is believed that no fee is due; however, should any fees under 37 C.F.R. §§ 1.16 to 1.21 be required for any reason, the Commissioner is authorized to deduct said fees from **Williams, Morgan & Amerson's P.C. Deposit Account 50-0786/2000.039500.**

Reconsideration of the application is respectfully requested.

REMARKS

In the Examiner's Answer to the Appeal Brief filed April 11. 2006, the Examiner entered multiple new grounds of rejection. Accordingly, Applicants respectfully request that prosecution be reopened and the following remarks be considered.

Claims 1-103 are pending in the present application.

In the Office Action, claims 1-38 and 51-103 were rejected under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention.

With regard to independent claim 1, the Examiner alleges that it is unclear whether the secret is removed from the first location. Applicant respectfully submits that independent claim 1 is not concerned with whether the secret is removed from the first location and therefore does not state whether or not the secret is removed from the first location. The Examiner also alleges that it is unclear whether the secret stored in the first location or the secret stored in the location different than the first location is used to retrieve the data stored in the first location. Applicant respectfully submits that copies of the same secret are stored in the first location and the location different than the first location. Therefore, independent claim 1 does not specify which location stores the copy of the secret that may be used to retrieve the data stored in the first location. Nevertheless, Applicant respectfully submits that the limitations that are set forth in independent claim 1 are clear.

With regard to independent claim 32, the Examiner alleges that it is unclear if the first location set forth in independent claim 32 is the same or different than the first location presented in independent claim 1. Applicant notes that claims 1 and 32 are independent claims and therefore the limitations set forth in these claims do not necessarily have any relation to each

other. However, Applicant notes that the limitations that are set forth in independent claim 32 are clear.

For at least the aforementioned reasons, Applicant respectfully submits that claims 1-38 and 51-103 are definite. Applicant requests that the Examiner's rejections of claims 1-38 and 51-103 under 35 U.S.C. § 112, second paragraph, be withdrawn.

In the Office Action, claims 1-103 were rejected under 35 U.S.C. § 102(e) as allegedly being obvious over Vu, et al (U.S. Patent No. 6,557,104) and Matthis (U.S. Patent Application Publication No. 2001/0037438). The Examiner's rejections are respectfully traversed.

Vu describes storing a cryptographic key, as well as a cryptographic program and any other data or information that may be required for the cryptographic processing, on a token, such as a magnetic strip, PCMCIA card, floppy disk, CD ROM, or any other similar removable storage device. *See* Vu, col. 4, ll. 21-36. The cryptographic key, the cryptographic program and other related data stored on the token may be loaded into a System Management RAM (SMRAM) and the SMRAM is then locked to prevent any other processes from accessing the data stored in the SMRAM. *See* Vu, col. 4, ll. 52-54. Once the cryptographic key has been stored in the SMRAM, the physical token is removed to ensure system integrity. *See* Vu, Col. 5, ll. 10-12. A security function may access the cryptographic key and programs stored in the SMRAM to perform security processing. *See* Vu, col. 5, ll. 35-37.

To establish a *prima facie* case of obviousness, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *In re Royka*, 490 F.2d 981, 180 U.S.P.Q. 580 (CCPA 1974). However, as admitted by the Examiner, Vu fails to teach or suggest retrieving at least a portion of the data stored in the first location using a secret read from a first location and stored in a secure location different than the first location, as set forth in

independent claims 1, 51, 55, and 66. Although Vu describes transferring a cryptographic program (and any other data or information that may be required for the cryptographic processing) from the physical token to the SMRAM, Vu does not teach that the cryptographic key is used to access the cryptographic program or any other data or information that may be stored on the physical token. To the contrary, the physical token that originally stored the cryptographic key must be removed to ensure system integrity, thereby preventing the system from accessing any data stored on the physical token after the cryptographic key has been transferred to the SMRAM. *See* Vu, Col. 5, ll. 10-12.

As also admitted by the Examiner, Vu fails to teach or suggest code stored in a first location and configured to provide access to data stored in the first location when processed in association with a secret stored in the first location, as set forth in independent claims 32, 64, and 97. The Examiner further admits that Vu fails to teach or suggest a master device configured to access data stored in the first location using a secret stored in the first location, as set forth in independent claim 39.

To attempt to remedy the acknowledged deficiencies of Vu, the Examiner alleges that Matthis describes retrieving or accessing data stored in a first location using a secret stored in a first location. Applicant respectfully disagrees. Matthis describes a secure memory device that is capable of reading binary content from a program memory device and computing a signature based on the binary content. The signature may be used to verify that the binary memory content has not been tampered with or otherwise compromised. The secure memory device may be coupled to the program memory device using a secure memory socket. See Matthis, paragraphs [0014-0200]. However, Matthis does not describe or suggest using a secret to access the binary content from the program memory device. To the contrary, Matthis teaches that the secure

memory device may directly access the binary content from the program memory device once the secure memory device is coupled to the secure memory socket.

Accordingly, Applicant respectfully submits that the cited references fail to teach or suggest all the limitations of the claimed invention. Furthermore, Applicant respectfully submits that the prior art of record fails to provide any suggestion or motivation for the Examiner's proposed combination and modification of the cited references. To the contrary, Vu teaches away from the present invention, as discussed below.

The Examiner identifies the physical token described by Vu as the "first location" and the SMRAM as the "secure location different than the first location." See Examiner's Answer, page 6. As discussed above, Vu teaches that data is accessed from the SMRAM, *i.e.*, the entity identified by the Examiner as the "secure location different than the first location," using the cryptographic key. Thus, Vu does not teach that the cryptographic key is used to access the cryptographic program or any other data or information that may be stored on the physical token. To the contrary, the cryptographic key is used to access information from the SMRAM and not from the physical token, *i.e.*, the "first location" identified by the Examiner. In fact, it is impossible to access information stored on the physical token because the physical token is removed to ensure system integrity once the cryptographic key has been stored in SMRAM. Accordingly, Vu teaches away from retrieving or accessing data stored in a first location using a secret stored in a first location.

It is by now well established that teaching away by the prior art constitutes *prima facie* evidence that the claimed invention is not obvious. *See, inter alia, In re Fine,* 5 U.S.P.Q.2d (BNA) 1596, 1599 (Fed. Cir. 1988); *In re Nielson*, 2 U.S.P.Q.2d (BNA) 1525, 1528 (Fed. Cir. 1987); *In re Hedges*, 228 U.S.P.Q. (BNA) 685, 687 (Fed. Cir. 1986).

For at least the aforementioned reasons, Applicant respectfully submits that the Examiner has failed to make a *prima facie* case that the present invention is obvious over Vu and Matthis. Applicant requests that the Examiner's rejections of claims 1-103 under 35 U.S.C. 103(a) be withdrawn

For the aforementioned reasons, it is respectfully submitted that all claims pending in the present application are in condition for allowance. The Examiner is invited to contact the undersigned at (713) 934-4052 with any questions, comments or suggestions relating to the referenced patent application.

Respectfully submitted,

Date: AUGUST 25, 2006

//MARK W. SINCELL//
Mark W. Sincell, Ph.D.
Reg. No. 52,226
Williams Morgan & Amerson, P.C.
10333 Richmond Avenue, Suite 1100
Houston, TX 77042
(713) 934-7000
(713) 934-7011 (Fax)

AGENT FOR APPLICANT